AEEC
Communications Security Activities

International CNS Conference
1 May 2007
Hilton Dulles Airport, Herndon, VA

Michael Olive – Honeywell International Inc.
Roy Oishi – ARINC
Stephen Arentz – United Airlines

ARINC UNITED Honeywell

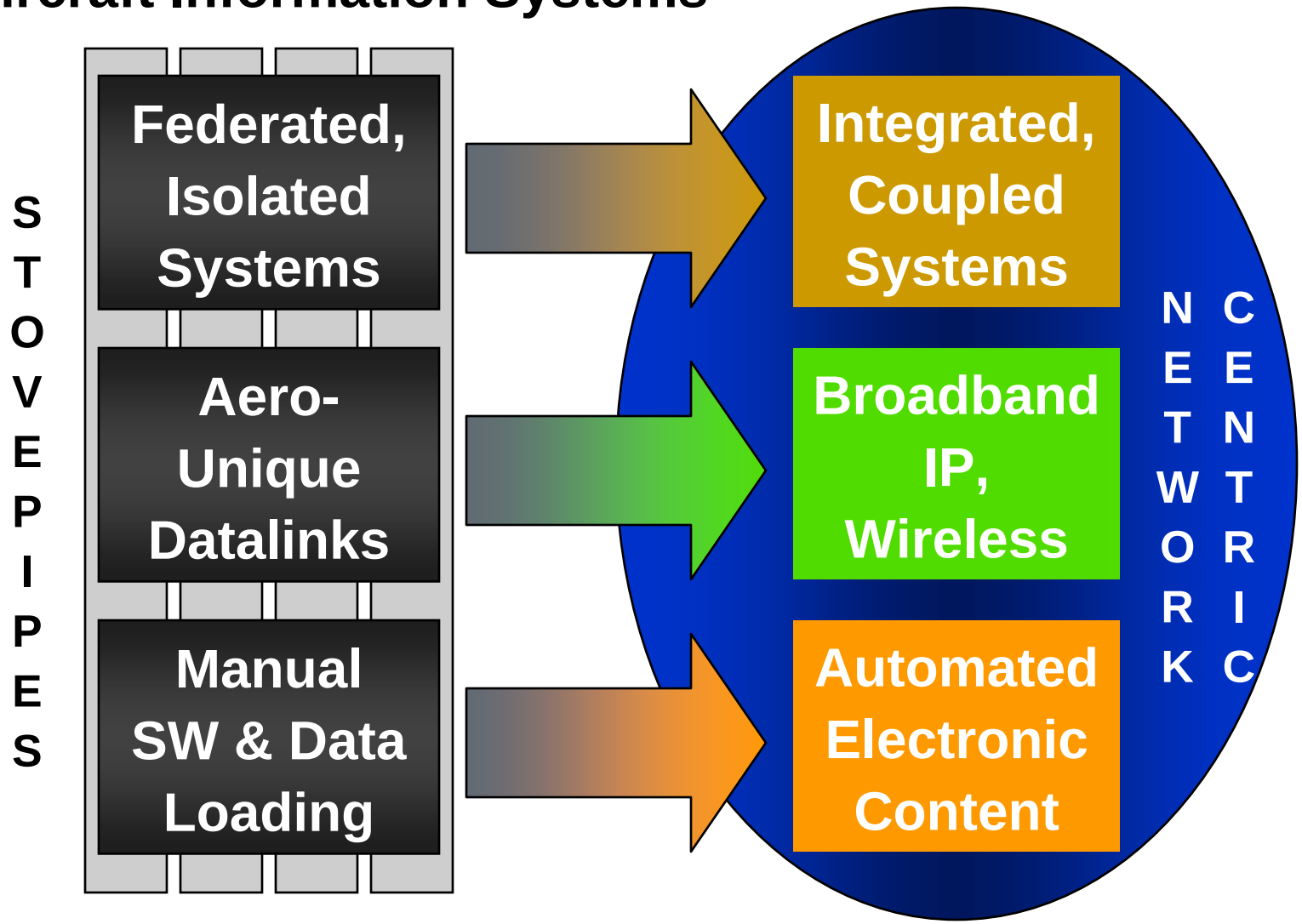
Content

ARINC
UNITED
Honeywell

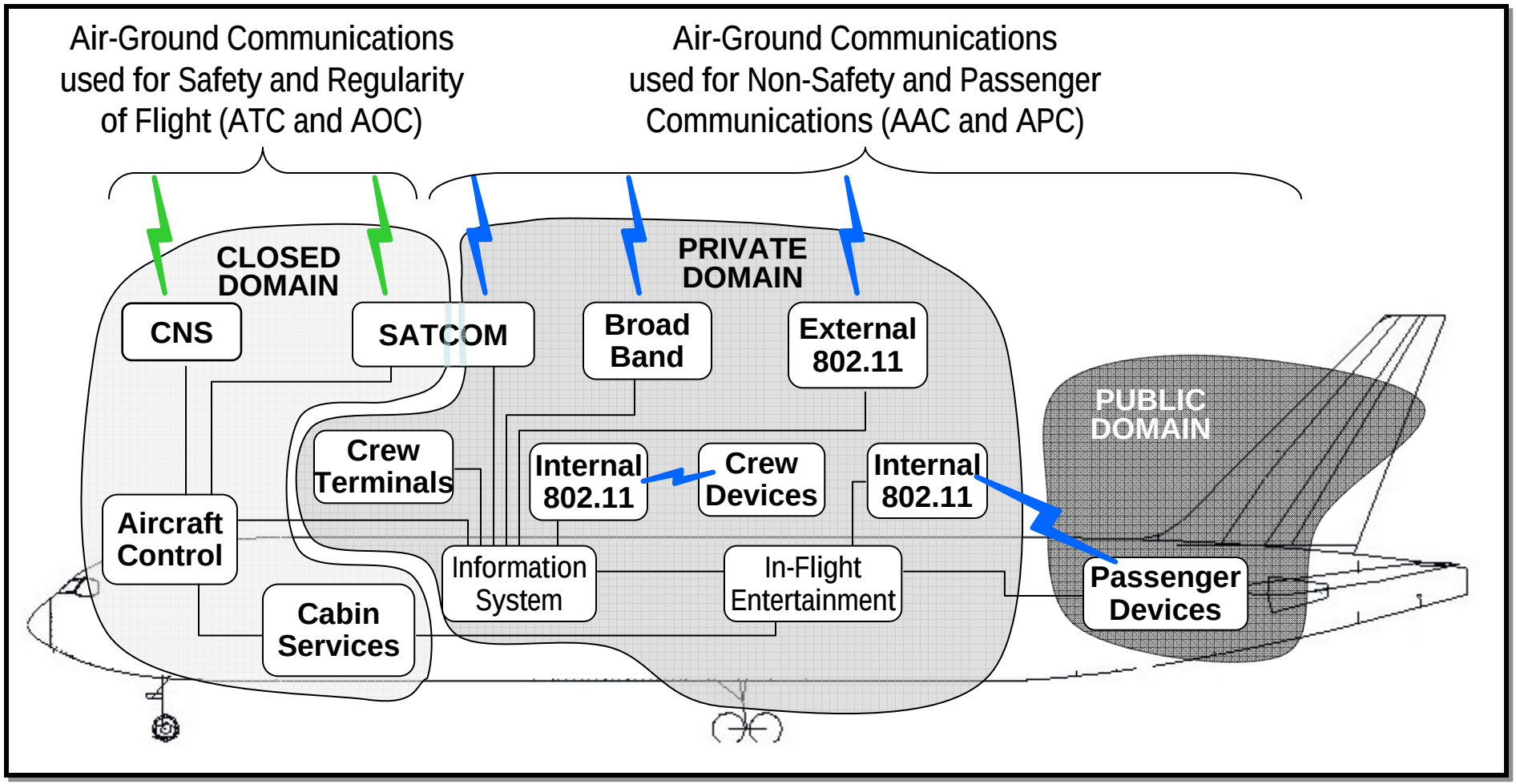
- **Background and Introduction**
- **Need for common methods and solutions**
  - **Dealing with Aircraft Domains: Aircraft as Network Node**
  - **Passenger, Airline, ATM: What overall network?**
  - **How many air-ground links can we afford?**
- **ARINC Report 811 – A Security Process Framework**
  - **Written for the airlines but framework is broadly applicable**
  - **Three-step process:**
    - Identify security needs and objectives
    - Select and implement controls
    - Operate and manage controls
- **Questions**

Introduction

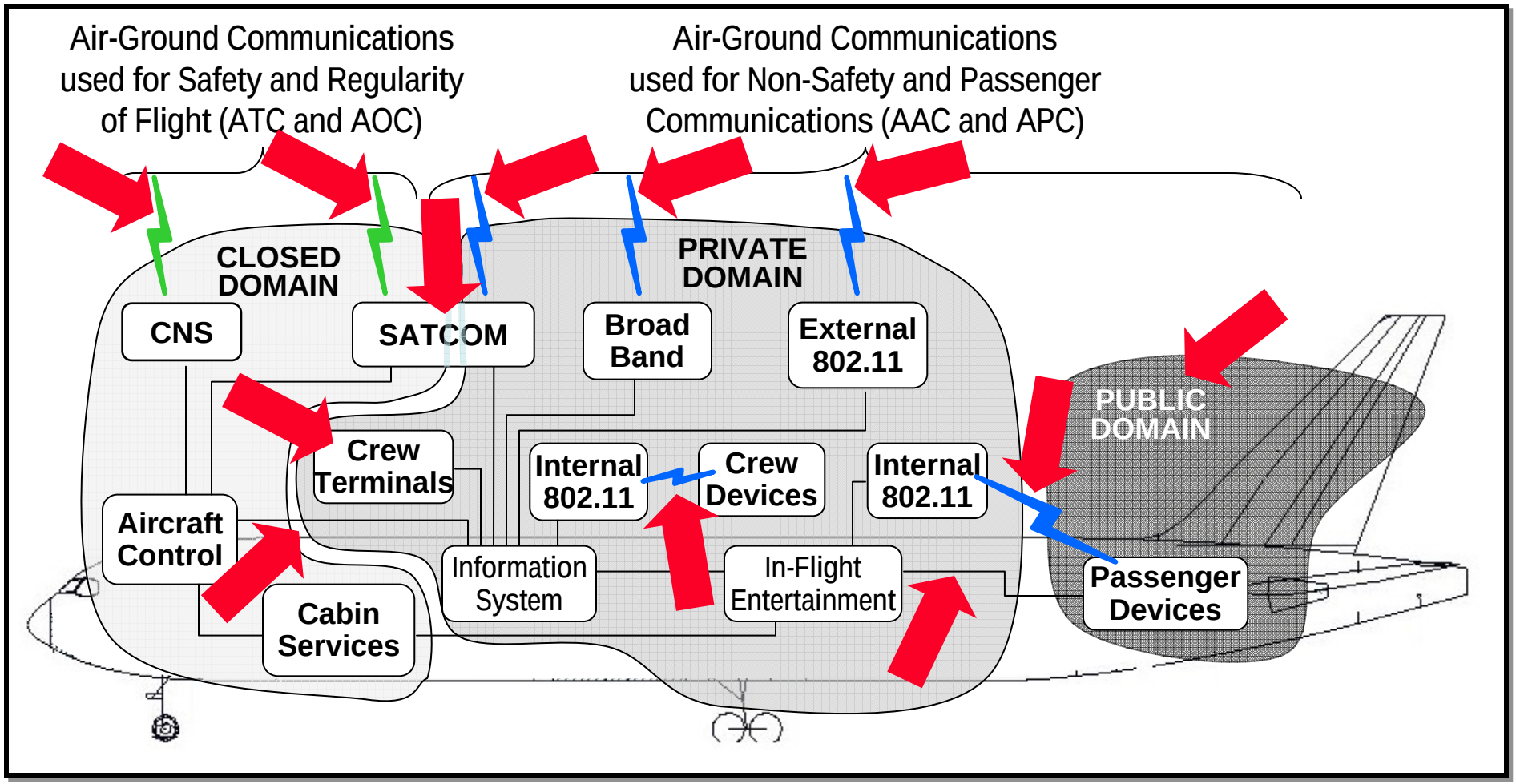
Impact of Information Technology on Airlines and Aircraft Information Systems



Networked Aircraft Information Systems



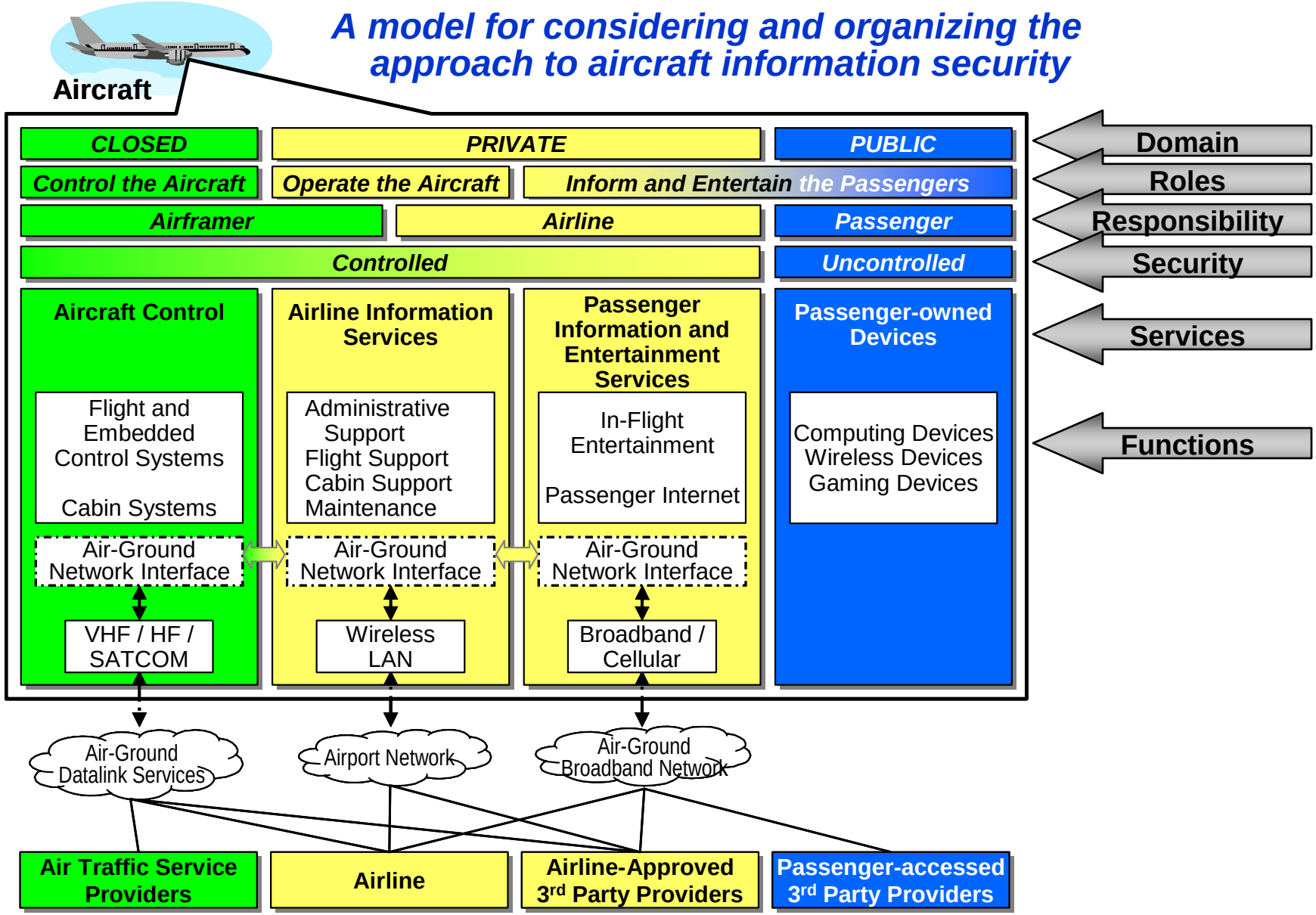
The Need for Aircraft Information Security



The ARINC 664 (ADN) Reference Model

ARINC
UNITED
Honeywell

A model for considering and organizing the approach to aircraft information security



AEEC Security Activities

- Long-standing Aircraft Data Network (ADN) SC working Ethernet issues
- Security (SEC) SC developed ARINC Report 811
- Cabin Systems SC (CSS) defined networking architecture for the cabin
- Data Link Systems (DLK) and Air-Ground Communications (AGCS) SCs working data link security
- Aircraft Network and File Server (ANFS) defining wireless gatelink
- Network Interfaces and Security (NIS) SC provides oversight

External Security Activities

ARINC
UNITED
Honeywell

- ICAO long ago defined SARPs for integrity and authentication requirements for ATN and requested AEEC to develop airline-specific guidance. Task still pending.
- ATA Digital Security WG (DSWG) developing common airline certificate policies
- Eurocae WG-72 developing security guidance
- Proposed RTCA security SC to develop means to deal with the problem of gaining security software approvals without ‘security cert’ process independent of the ‘safety cert’ process.

The Need for Standardization

ARINC
UNITED
Honeywell

- **Aircraft Information Security is too complex for any one organization**
  - Global operations
  - Aircraft Mobility
  - Numbers and Types of Aircraft and Equipment
  - Differing network and security requirements
- **Each involved organization needs standardized approaches**
  - To effectively manage all configurations
  - To reduce confusion and conflicts
- **Aero Organizations and Industry Standards groups are independently identifying information security needs**
  - Risk of stovepipe information security solutions
  - AEEC, ATA, Eurocae, ICAO, airframe manufacturers

Need for Common Solutions

ARINC
UNITED
Honeywell

- **Any good security system will be expensive to implement**
- **Airlines are already attempting to integrate ground IT security solutions with the aircraft, but...**
  - **Software on the aircraft has to have safety evaluations**
  - **Security controls cannot be different for each application as the result will be unmanageable and cost prohibitive**
  - **The range of different applications will inevitably grow**

When two-way air-ground data communications are needed for ATM, a unique security solution will not be affordable either for ANSPs or for aircraft operators or for avionics vendors or for communications networks

ARINC Report 811 Overview [1/2]

ARINC
UNITED
Honeywell

- **ARINC 811 – *Commercial Aircraft Information Security Concept of Operations and Process Framework***
  - **Work product of the Airlines Electronic Engineering Committee (AEEC) Aircraft Information Security (SEC) Sub-committee**
  - **Adopted October 2005**
  - **Published December 2005**
  - **Available from ARINC (www.arinc.com)**
- **What the document does:**
  - **Facilitate an understanding of aircraft information security**
  - **Present aircraft information security operational concepts**
  - **While written for the airlines, it describes a generic security framework that can be applied elsewhere**
- **What the document does not:**
  - **Attempt to solve specific application, communication, or network security issues**

ARINC Report 811 Overview [2/2]

ARINC
UNITED
Honeywell

ARINC 811 – Commercial Aircraft Information Security Concepts of Operation and Process Framework

Main Body	Attachment 1	Attachment 2	Attachment 3
	Glossary And Acronyms	Airline Operational Overview	Aircraft Info. Security Process Framework & Examples

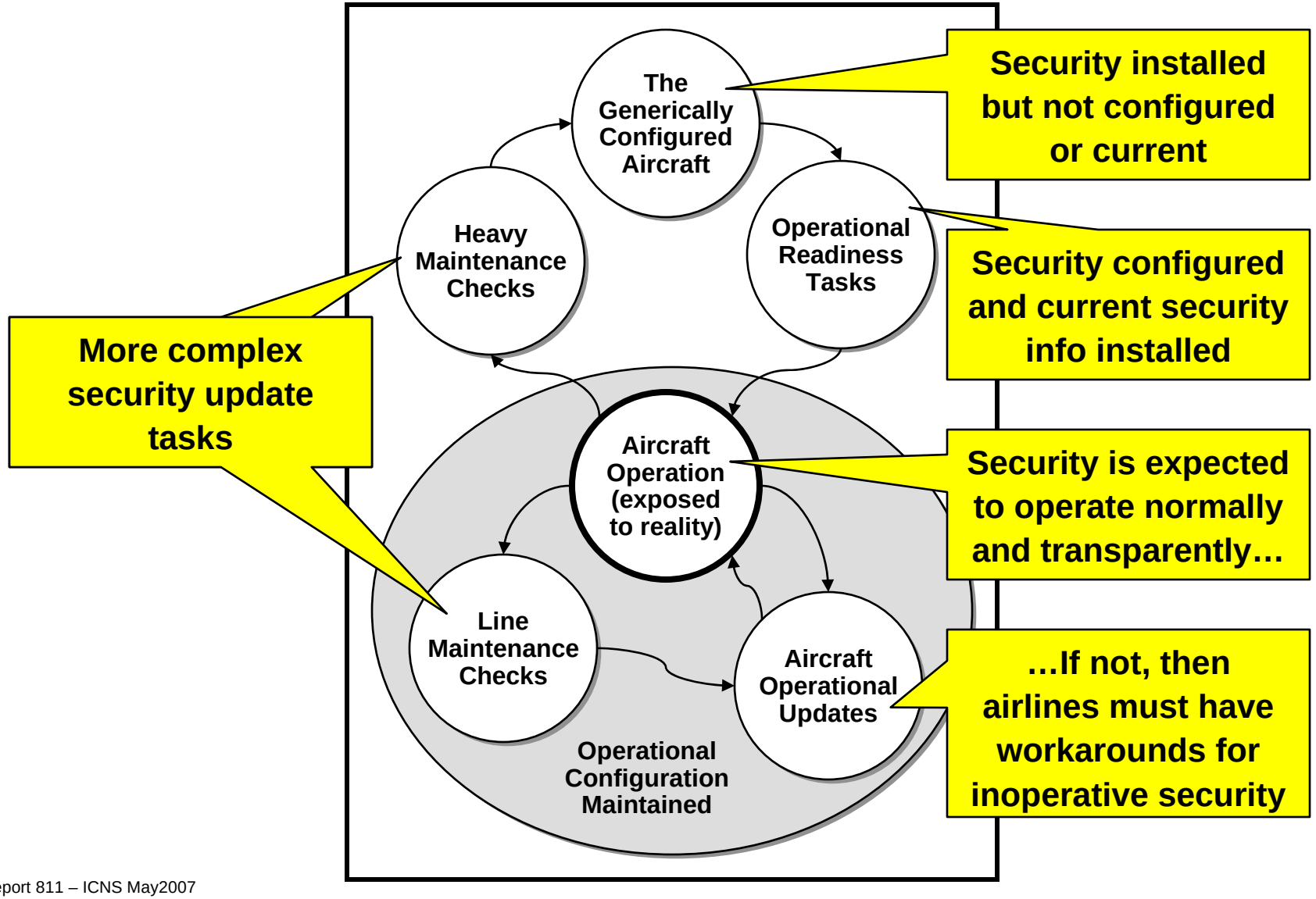
- ~20 pages
- Introduction
- How to read document
- Attachment summary
- Recommendations to AEEC Subcommittees
- Recommendations to Airlines

- ~20 pages
- Describes existing airline operating environment
- Provides real-life context for aircraft information security

- ~90 pages
- Presents a high-level risk-based information security process framework for selecting and implementing minimum security controls in a consistent manner based on airline needs and policies

Airline Operational Perspective

Aircraft Life Cycle Considerations



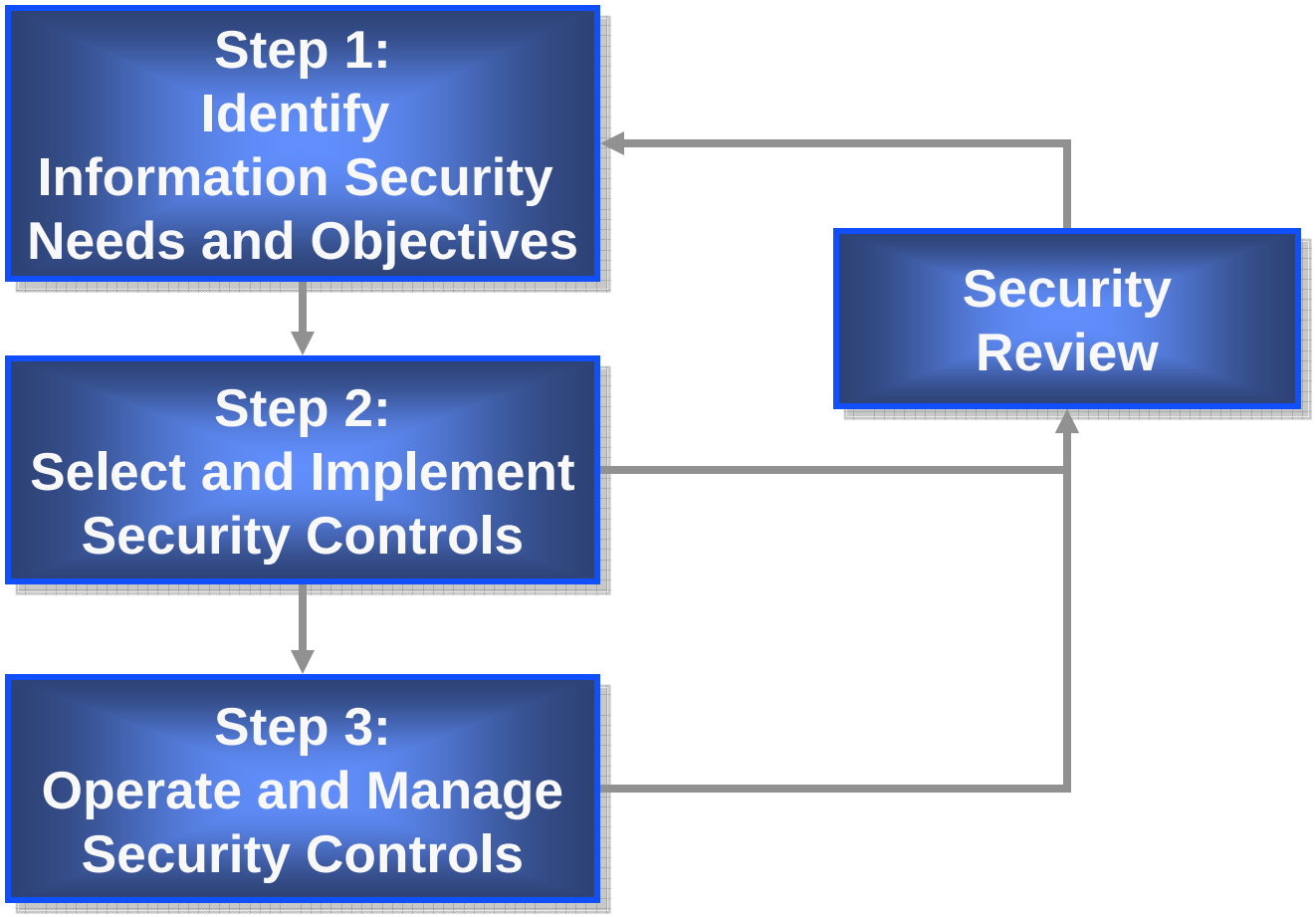
The ARINC 811 Aircraft Information Security Process Framework

ARINC
UNITED
Honeywell

- A high-level, risk-based information security process
- That is applicable to aircraft information systems
- That offers an approach to identify, assess, and mitigate information security risks
- That allows organizations the ability to:
  - Integrate with existing business/operational life cycle processes
  - Tailor to suit individual business/operational objectives
  - Apply in a consistent and repeatable manner

Information Security Process Overview [1/2]

High-level Information Security Process Steps



Information Security Process Overview [2/2]

ARINC
UNITED
Honeywell

MANAGEMENT CONTROLS
Processes that are performed by an organization to maintain risk to an acceptable level

- Risk Assessment
- Planning
- System & Services Acquisition
- Certification, Accreditation, and Assessment

OPERATIONAL CONTROLS
Processes that are performed by people

- Personnel Security
- Awareness/Training
- Physical / Environmental Protection
- Contingency Planning
- Incident Response
- Configuration Mgmt
- Maintenance
- System & Info Integrity
- Media Protection

TECHNICAL CONTROLS
Mechanisms that are implemented primarily in hardware, software or firmware

- Identification and Authentication
- Access Control
- Audit and Accountability
- System & Comms. Protections

Reference NIST 800-53, which provides a cross reference to ISO 17799

Practical Applications of ARINC 811

ARINC
UNITED
Honeywell

AEEC Datalink Security (DSEC) Subcommittee

- During first DSEC meeting, engaged participants in Step 1 of the security process
  - Datalink information assets identified and categorized
  - Preliminary risk assessment performed
  - Security objectives identified and prioritized
- Results documented in PP823 Part 1

EuroCAE WG-72 – Aeronautical System Security

- Developing guidance material for manufacturers and airworthiness/regulatory authorities
- Guidance to include a high-level Air Transportation System Security Reference Model
  - SEC representatives have encouraged WG-72 to use Step 1 of the process to identify and categorize assets

Acknowledgement

This presentation draw extensively from material contained in ARINC Report 811. The authors gratefully acknowledge the contributions of the AEEC Aircraft Information Security (SEC) subcommittee participants to the development of the ARINC Report 811 document.

Questions

Background Information

Airline Operational Perspective [2/2]

ARINC
UNITED
Honeywell

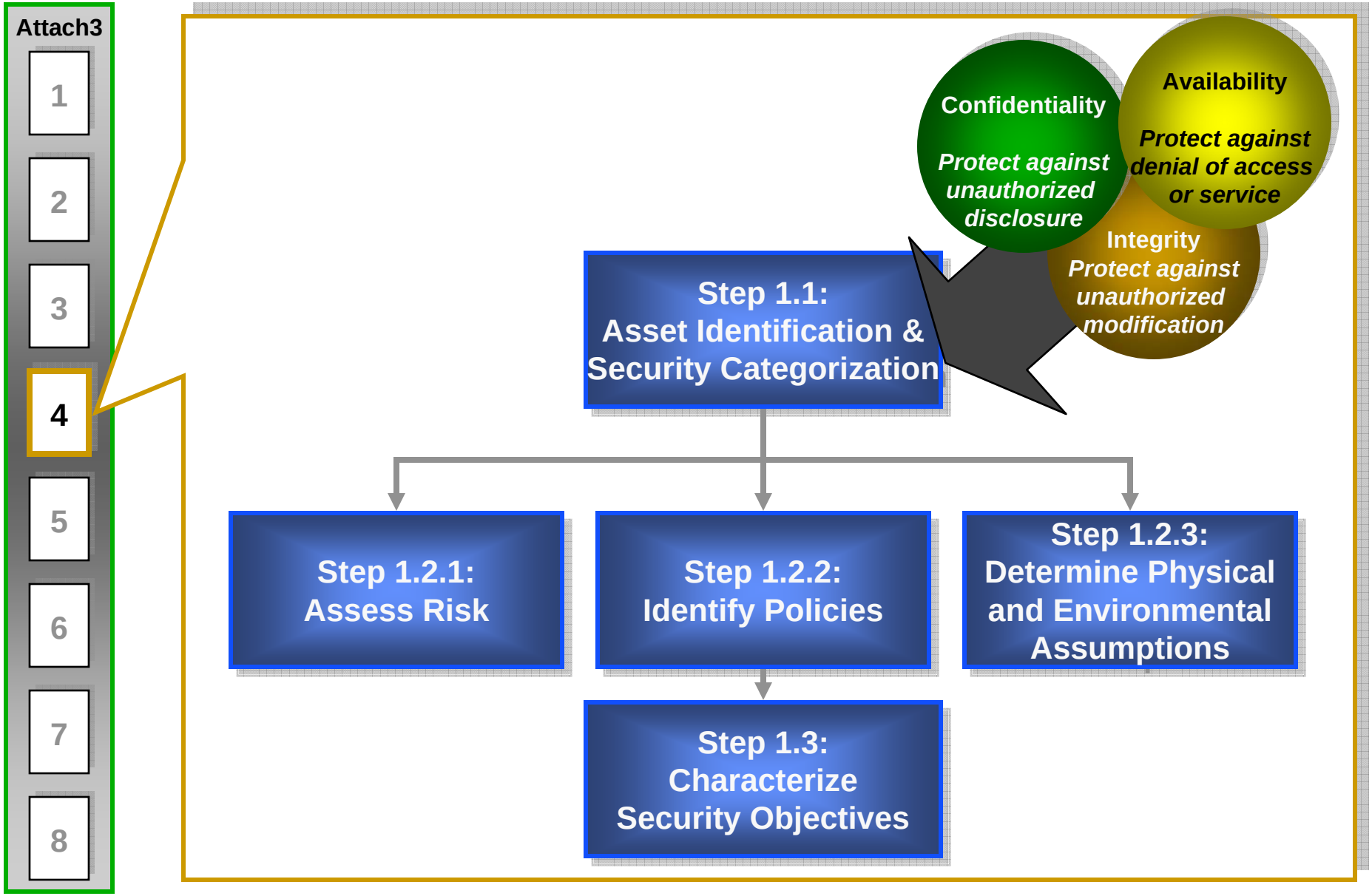
Aircraft Operating Mode Considerations

- Aircraft may be in one of three modes:
  - Normal
  - Non-normal (e.g., failure)
  - Maintenance
- Aircraft modes overlay life cycle states

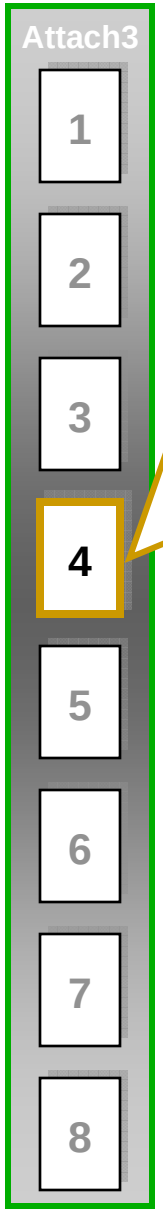
Integrating New Security Roles

- Today aircraft mechanics “touch” the aircraft, not IT
- Definition of generic security roles is needed
  - Provides equipment and service providers with an abstraction layer for security roles/responsibilities
  - Provides airlines with flexibility to assign roles based on its organizational structure

Step 1: Identify InfoSec Needs and Objectives [1/2]

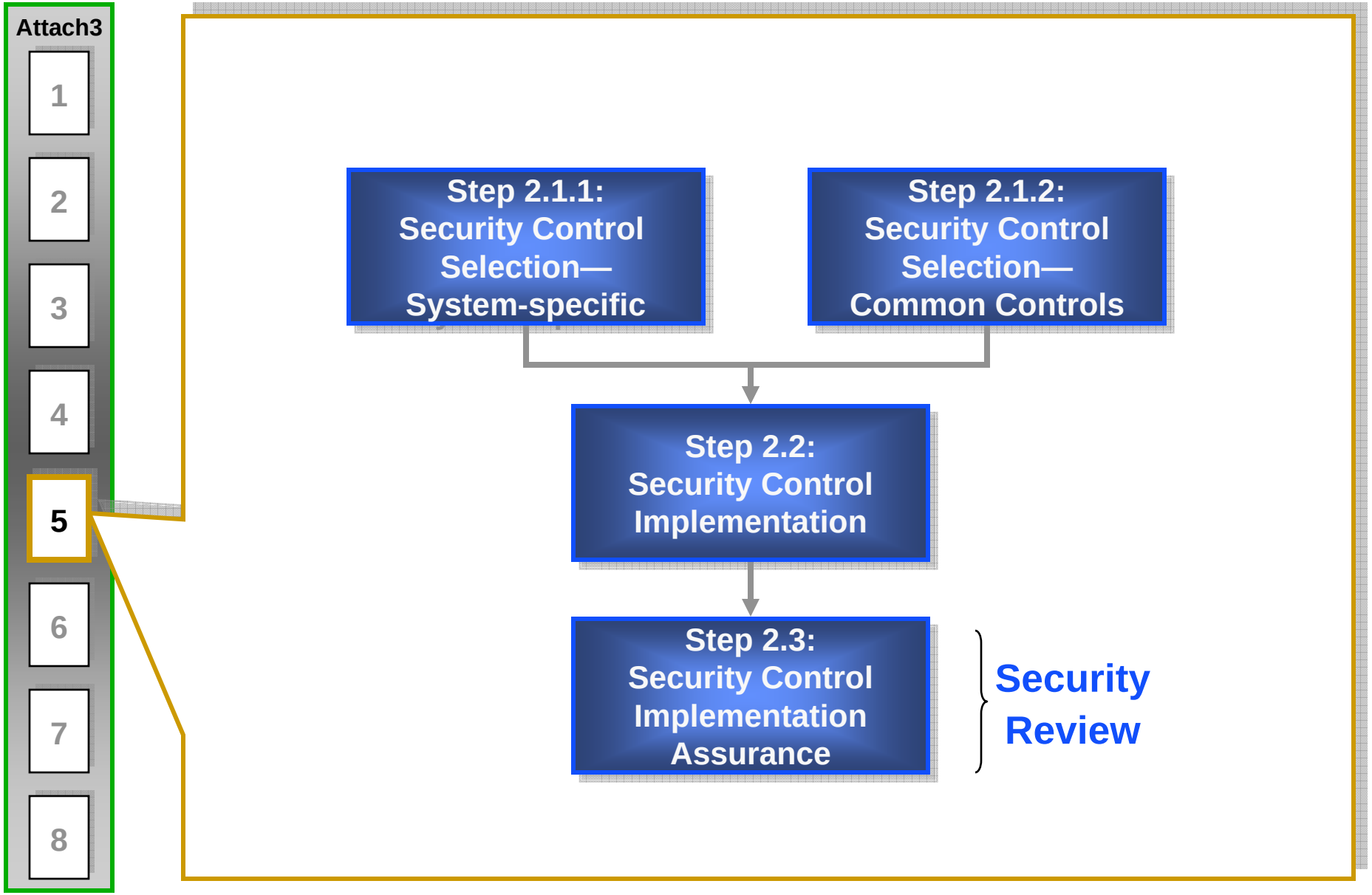


Step 1: Identify InfoSec Needs and Objectives [2/2]



- **Use common security controls to the greatest extent possible.**
- **Minimize Overall Cost.**
- **Avoid Reliance on singular security controls (Defense-in-depth).**
- **Respect aircraft configuration-lifecycle, operational-states, modes.**
- **Require as few changes as possible to existing systems.**
- **Be flexible.**
- **Provide effective operation to users performing authorized actions.**
- **Allow for regular adoption of new security controls and technology.**
- **Require minimal administrative and operational overhead.**
- **Not inhibit or degrade airline mission accomplishment.**
- **Use open standards.**
- **Protect from threats that may affect industry commercial image.**
- **Do Not compromise the safety of the aircraft.**
- **Mitigate the risks to an acceptable level.**

Step 2: Select & Implement Security Controls [1/2]



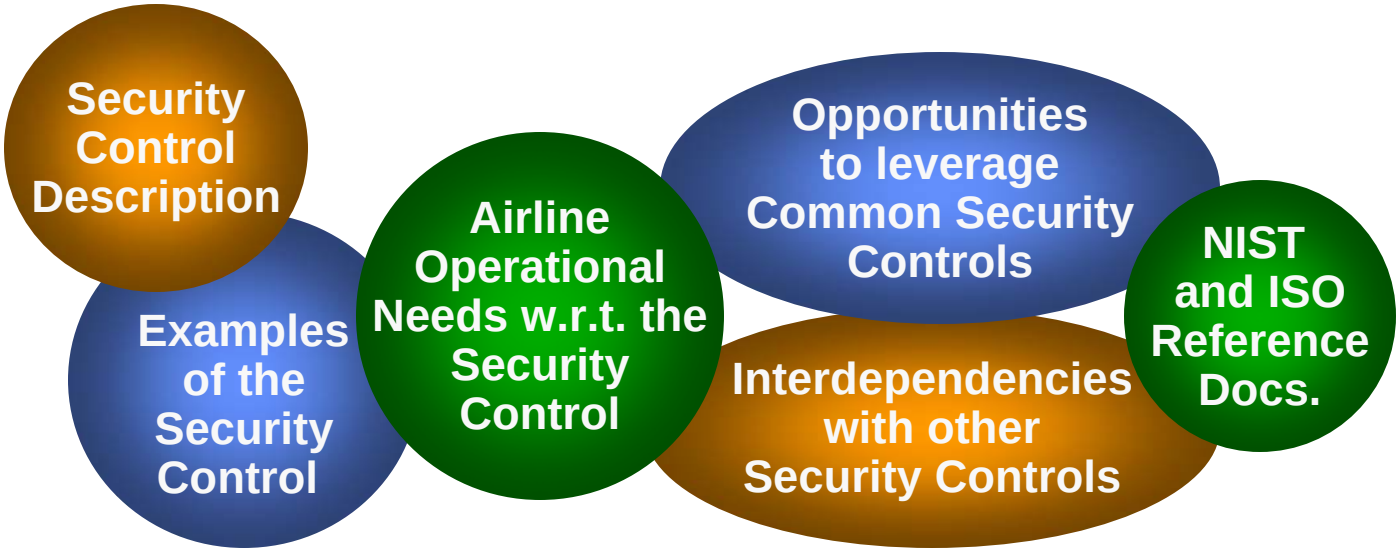
Step 2: Select & Implement Security Controls [2/2]

ARINC UNITED Honeywell

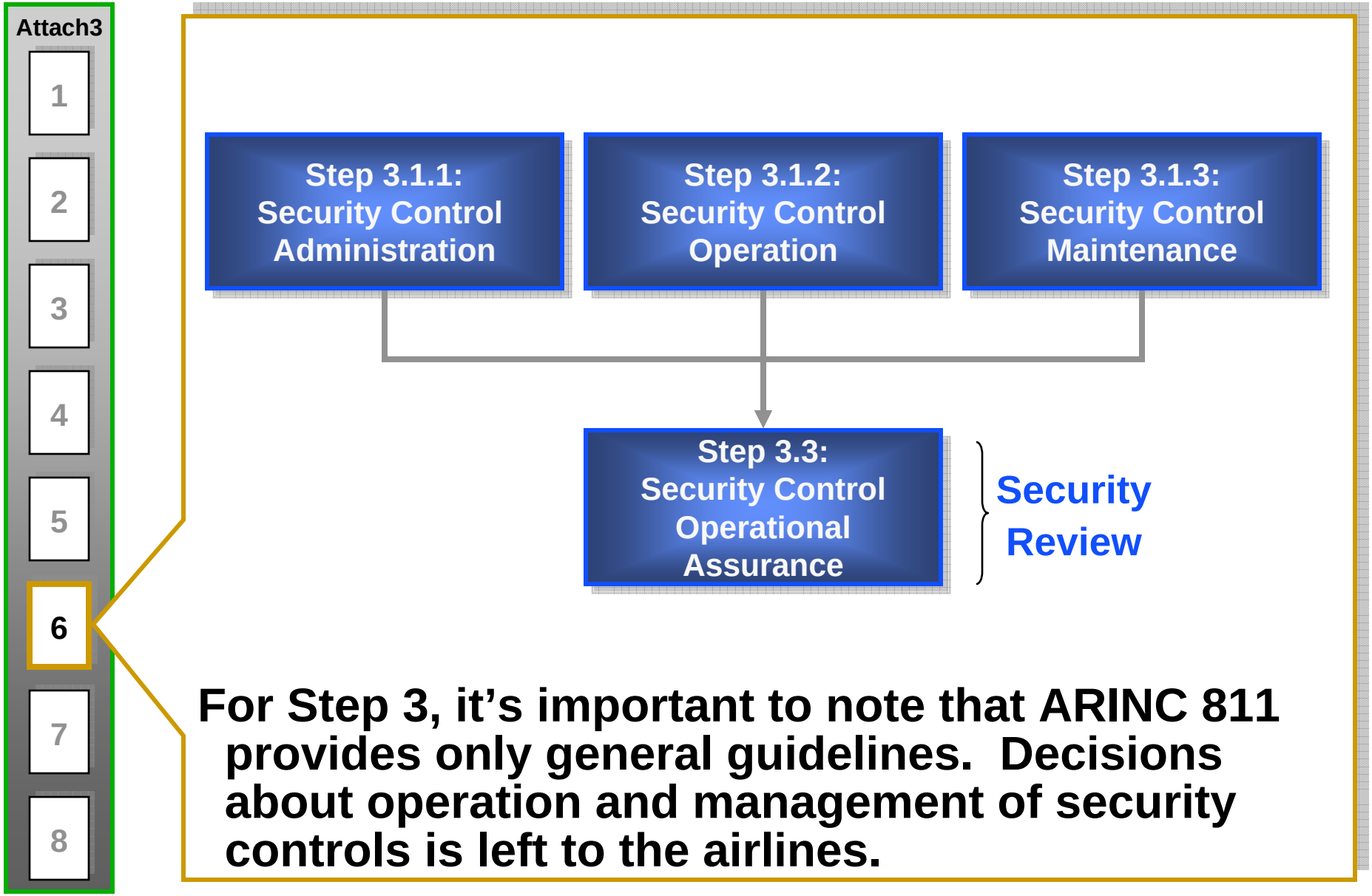
Attach3

1
2
3
4
5
6
7
8

- **Presented in terms of the 17 high-level security controls identified in NIST 800-53**
- **Each security control addresses implementation considerations driven by airline operational needs**



Step 3: Operate & Manage Security Controls



For Step 3, it's important to note that ARINC 811 provides only general guidelines. Decisions about operation and management of security controls is left to the airlines.